REMARKS

This communication is responsive to the Final Office Action dated August 23, 2006 and received in this application. Claims 1-24 and 35-46 are pending in the application. Reconsideration of the pending claims is respectfully requested in light of the following remarks.

Claims 1-9, 13-21 and 35-42 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky") in view of B. Schneier, "Applied Cryptography," John Wiley & Sons, 1996, pp. 33-34 ("Schneier II"). This rejection is traversed.

Independent claim 1 recites: *[a]n authentication system, said authentication system comprising:*

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification

information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

Applicant appreciates the indication that the Examiner found the previously submitted remarks persuasive, in reconsidering and withdrawing the previous rejection of record, which was reliant upon pages 170-178 of the Schneier book. However, Applicant submits that the pages of Schneier II are also deficient with regard to the claimed invention, and requests reconsideration and withdrawal of the new grounds of rejection in that regard.

As previously discussed, Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security. Nemirofsky makes no mention of encrypting the PIN code.

The previously relied upon Schneier reference discloses that it is known to generate encryption keys, and that these keys are used to encrypt sensitive information that is sent between parties or devices. Applicant submits that Schneier II makes similar disclosures, and also does not cure the deficiencies of Nemirofsky.

Before addressing Schneier II, Applicant notes that claim 1 entails authentication features involving the first identification information (*e.g.*, the portable card terminal ID), correlated generation of an encryption key, and encryption of second identification information input to the portable card terminal using the encryption key. Specifically, the claim recites an authentication system wherein, among other things, (1) the "first identification information" (card ID) is sent from the portable card terminal to the authentication device, (2) the authentication device generates the encryption key and sends it back to the portable terminal device, and (3) the portable terminal device then uses the encryption key to encrypt the second identification information input to the portable card terminal (*e.g.*, the PIN entered by the user) and send this encrypted second identification information to the authentication device, which then performs authentication.

Nemirofsky does not disclose various aspects of this sequence. Nemirofsky does disclose a smart card, and discloses that a PIN may be used, but makes no mention with regard to any encryption technique for that PIN, let alone the particular sequence claimed by Applicant. The Examiner generally refers to "pages 33-34" of Schneier, but Applicant does not believe that anything contained therein discloses the claimed features as noted above. On page 33 of Schneier II, public-key cryptography, and particularly an example of a "hybrid cryptosystem" is described. This description does not disclose or suggest Applicant's claimed invention. With regard to this, Schneier II offers the following example:

> "(1) Bob sends Alice his public key
>
> (2) Alice generates a random session key, K, encrypts it using Bob's public key, and sends it to Bob. $E_B(K)$
>
> (3) Bob decrypts Alice's message using his private key to recover the session key. $D_B(E_B(K))=K$

(4) Both of them encrypt their communications using the same session key."

(Schneier II, at p. 33).

This is clearly distinct from, and offers no disclosure or suggestion of the particular features claimed by Applicant. The disclosed technique offers a way to send an encrypted session key from user A to user B, with user B being able to decrypt the session key using a private key. There is no disclosure of the particular authentication features claimed by Applicant. With Applicant's claimed invention the card ID is sent to the authentication device, then the authentication device generates the encryption key information and forwards the so-generated encryption key information to the portable card terminal. Only then does the portable card terminal encrypt the second identification information that has been input, using the so-generated encryption key information. There is no disclosure or suggestion of these particular features of Applicant's claimed invention, even in the combination proposed by the Examiner.

The Examiner has previously cited Nemirofsky's disclosure of a smart card serial number as a possible portable card identifier as claimed. However, even assuming this to be correct, there still would be no disclosure or suggestion of the claimed authentication features. Applicant reiterates that concluding as such would require significant conjecture, even in light of Schneier II. That is, one would have to conclude that the smart card serial number is sent out, that an encryption key is then generated and then returned to the smart card, with the smart card then using that encryption key to encrypt the PIN number. Given that Nemirofsky does not even generally disclose encrypting the PIN number, it cannot be fairly concluded that the disclosure of public-key cryptography techniques by Schneier II would disclose, suggest, or in any way motivate the artisan to provide such features. That is, Schneier II discloses receipt of a public key, which is used to encrypt a session key, and corresponding decryption of the session key based upon a previously held private key. These features do not disclose or suggest generating and returning an encryption key in association with a received portable card terminal identifier, and then encrypting second information that is input to the portable card terminal using the so-generated encryption key.

Page 33 of Schneier II thus clearly fails to remedy the deficiencies of Nemirofsky. In

fact, Applicant believes that Schneier II teaches away from Applicant's claimed invention. With regard to public-key algorithms, Schneier II states that:

> "[i]n the real world, public-key algorithms are not a substitute for symmetric algorithms. They are not used to encrypt messages, they are used to encrypt keys."

(Schneier II, at p. 33).

Thus, in addition to failing to specify the sequence that is absent from Nemirofsky, Schneier II suggests that the disclosed public-key algorithms are not even relevant to the type of information that is encrypted in accordance with Applicant's claimed invention. That is, with Applicant's claimed invention, information that is input to the portable card terminal is encrypted. This is clearly in contrast, even generally, to the encryption of a session key.

The afore-mentioned Merkle's Puzzles of page 34 of the reference also fail to offer any disclosure that would suggest Applicant's claimed invention. These puzzles merely appear to offer a way to illustrate the difficulty of breaking particular encryption techniques, based upon the number of iterations it would require an "eavesdropper" to recover an encrypted message. There is no mention whatsoever regarding the above-described features of Applicant's claimed invention.

Applicant submits that a *prima facie* case of obviousness remains absent for independent claim 1. The other independent claims are also neither disclosed nor suggested by the combination of Nemirofsky and Schneier II, for reasons similar to those provided regarding claim 1, as they have been similarly amended. The claims depending from these claims are also neither disclosed nor suggested by the relied upon references, for their respective incorporation of the features recited in the independent claims, as well as their separately recited, patentably distinct features.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-9, 13-21 and 35-42 under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II.

Claims 10-12, 22-24 and 43-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of Lillibridge. This

rejection is traversed.

For reasons already of record, Lillibridge does not remedy the deficiencies of Nemirofsky and Schneier II as described above. Lillibridge appears to disclose a string that may be randomly modified to form a riddle, and offers no disclosure or suggestion of the features recited in Applicant's independent claims.

The claims are thus still neither disclosed nor suggested by the three reference combination of Nemirofsky, Schneier II, and Lillibridge. The dependent claims are also neither disclosed nor suggested by the relied upon references, for their respective incorporation of the features recited in the independent claims, as well as their separately recited, patentably distinct features.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of Lillibridge.

For the foregoing reasons, reconsideration and allowance of the claims which remain in this application are solicited. If any further issues remain, the Examiner is invited to telephone Christopher M. Tobin at (202) 955-8779 to resolve them.

Dated: Oct. 16, 2006

Respectfully submitted,

By _____ 40,290

Ronald P. Kananen
Registration No.: 24,104
Christopher M. Tobin
Registration No.: 40,290
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building, 1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750; Fax: (202) 955-3751
Customer No. 23353